Robustness of two-way quantum communication protocols against Trojan horse attack

Fu-Guo Deng,[1,2,3] Ping Zhou,[1,2] Xi-Han Li,[1,2] Chun-Yan Li,[1,2] and Hong-Yu Zhou[1,2,3]
[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, China*
[3] *Beijing Radiation Center, Beijing 100875, China*

(Dated: February 1, 2008)

We discuss the robustness of two-way quantum communication protocols against Trojan horse attack and introduce a novel attack, delay-photon Trojan horse attack. Moreover, we present a practical way for two-way quantum communication protocols to prevent the eavesdropper from stealing the information transmitted with Trojan horse attacks. It means that two-way quantum communication protocols is also secure in a practical application.

PACS numbers: 03.67.Hk, 03.67.Dd

Quantum communication supplies some novel ways for the transmission of message, such as quantum key distribution (QKD) [1, 2, 3, 4, 5, 6, 7], quantum secure direct communication (QSDC) [8, 9, 10, 11, 12, 13, 14, 15, 16, 17], quantum secret sharing (QSS) [18, 19, 20, 21, 22, 23, 24, 25, 26, 27], and so on. QKD provides a secure way for creating a private key with which two remote parties, say Alice and Bob, can communicate in an unconditionally secure way even though an eavesdropper, Eve is monitoring the channel. After Bennett and Brassard published their pioneering work [1] in 1984, called BB84, QKD attracts a lot of attentions [1, 2, 3, 4, 5, 6, 7] and becomes one of the most mature applications of quantum information.

QSS and QSDC are two important branches of quantum communication, and have been developing quickly in recent years. QSS is the generalization of classical secret sharing [28] into quantum scenario and supplies a secure way for sharing both a piece of classical information [18, 19, 20, 21, 22, 23] and quantum information [24, 25, 26, 27]. The gents can obtain the message sent by the sender only when they cooperate, otherwise they can get nothing. QSDC is used to transmit the secret message directly [8, 9, 10, 11, 12, 13, 14] without creating a private key and then encrypting the message.

Recently, there are some two-way protocols proposed for QKD [5, 6, 7], QSS [20, 27], and QSDC [8, 9, 10, 11, 12, 13, 14]. Although there are differences among particular quantum communication protocols, almost all of them include the following procedures [5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 20, 27]. First, the receiver of information, say Bob, prepares the quantum signal randomly in one of some nonorthogonal states or a mixed state, and sends it to the sender Alice. Alice chooses one of two modes, checking mode and coding mode, to deal with the quantum signal. If Alice chooses the checking mode, she will obtain a sample for eavesdropping check with the measurement on the signal, otherwise she operates the signal with local unitary operations and sends it back to Bob. Bob measures the signal and gets the information transmitted by Alice. There are at least two transmissions of the quantum signal, i.e., from Bob to Alice, and from Alice to Bob. These two-way quantum communication protocols can be attacked with a Trojan horse if the two parties use only a simple way for eavesdropping check. On the other hand, this class of attacks can be detected with a little of modification in the eavesdropping checks. In this paper, we will discuss three types of Trojan horse attacks on two-way quantum communication protocols and present a way for improving their security against those attacks with a photon number splitter (PNS: 50/50) and a wavelength filter.

The typical two-way quantum key distribution protocol can be described as follows with polarized single photons [5, 6].

(1) Bob prepares a polarized single photon in one of the four states $\{|+z\rangle, |-z\rangle, |+x\rangle, |-x\rangle\}$ randomly. Here

$$|+z\rangle = |0\rangle, \tag{1}$$

$$|-z\rangle = |1\rangle, \tag{2}$$

$$|+x\rangle = \frac{1}{2}(|0\rangle + |1\rangle), \tag{3}$$

$$|-x\rangle = \frac{1}{2}(|0\rangle - |1\rangle), \tag{4}$$

and $\{|+z\rangle, |-z\rangle\}$ are the two eigenstates of σ_z, and $\{|+x\rangle, |-x\rangle\}$ are those of σ_x.

(2) Bob sends the photon to Alice, and Alice chooses one of the two modes to deal with it. If she chooses checking mode, Alice measures the photon with one of the two measuring bases (MBs), σ_z and σ_x, randomly. If she chooses the coding mode, she operates the photon with one of the two unitary operations I and U. Here $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ is the identity matrix and $U = |0\rangle\langle 1| - |1\rangle\langle 0|$. The nice feature of the U operation [5, 9] is that it flips the state in both measuring bases, i,e,

$$U\{|+z\rangle, |-z\rangle\} = \{-|-z\rangle, |+z\rangle\}, \tag{5}$$

$$U\{|+x\rangle, |-x\rangle\} = \{|-x\rangle, -|+x\rangle\}. \tag{6}$$

(3) Alice sends the photon operated to Bob, and Bob measures it with the same MB as that he prepares it.

(4) Alice and Bob repeat the process until they obtain enough key bits.

(5) Alice and Bob analyze the error rate of the samples obtained with the checking mode. Moreover they pick out randomly a subset of the outcomes obtained by Bob for eavesdropping check.

(6) If they can determine that the quantum channel is secure, they do error correction and privacy amplification on the outcomes to distill a private key.

In fact, this QKD protocol is equivalent to two BB84 QKD protocol if the eavesdropper Eve does not attack it with a Trojan horse. The latter is proven unconditionally secure [29]. If the QKD protocol is robust against Trojan horse attacks, it is also secure.

Now, let us introduce the three types of Trojan horse attacks. The first one is the general Trojan horse attack introduced in Ref. [2]. That is, Eve sends a light pulse to Alice, same as Bob. The second is a new one, the delay-photon Trojan horse attack. In detail, Eve intercepts the signal transmitted from Bob to Alice, and then inserts a fake photon in the signal with a delay time, shorter than the time windows [2]. In this way, Alice cannot detect this fake photon as it does not click Alice's detector. After the operation done by Alice, Eve intercepts the signal again and separates the fake photon. She can get the full information about Alice's operation with measurement. The third Trojan horse attack is the invisible photon attack proposed by Cai recently [30]. Its main idea is that Eve inserts an invisible photon in each signal prepared by Bob and sends it to Alice. As Alice's detector cannot click this photon and performs an unitary operation on each signal, Eve can steal the information about Alice's operation by means that she intercepts the signal operated and separates the invisible photon from each signal. With the measurement on the invisible photon, Eve can read out Alice's information. Its implement may be resort to the second attack strategy as it is necessary for Eve to separate the invisible photon from the signal without destroying the original photon.

In essence, the security of quantum communication protocol comes from the fact that the authorized users can detect the eavesdropper with measurements on some samples. For the third Trojan horse attack proposed by Cai [30], Alice needs only to add a wavelength filter [2] on each signal before she deals with it (i.e. coding or measuring it). In practical quantum communication, Alice and Bob should exploit a wavelength filter to filtering the light from background, in particular in free space. So there is no problem for the users to deal with this attack.

For the delay-photon Trojan horse attack, Alice should use a PNS to divide each sample signal into two pieces and measure them with two MBs. If there is only one photon in the original signal, Alice can only get one outcome, otherwise she will obtain two outcomes. In this way, Alice can improve the security of two-way quantum communication protocols against the Trojan horse attacks. Obviously, the method is also efficient for Alice to avoid the first Trojan horse attack. In practical, photon number splitting technique is not easy to be implemented with current technology [2], a photon beam splitter (PBS: 50/50) which is not difficult to be made can be used to replace the PNS . If the time windows of the two single-photon devices is long enough, Alice can detect the eavesdropping with a multi-photon fake signal.

In summary, a PBS and a wavelength filter can be used to avoid the two-way quantum key distribution protocol against Trojan horse attacks. The same result can be drawn for the other two-way quantum communication protocols, such as QSS [20, 27] and QSDC [8, 9, 10, 11, 12, 13, 14] protocols.

This work is supported by the National Natural Science Foundation of China under Grant Nos. 10447106, 10435020, 10254002, and A0325401, and Beijing Education Committee under Grant No. XK100270454.

[1] C. H. Bennett and G. Brassad, *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing, Bangalore*, India (IEEE, New York, 1984), PP.175-179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] G. L. Long and X. S. Liu, Phys. Rev. A **65**, 022317 (2002).

[4] F. G. Deng and G. L. Long, Phys. Rev. A **68**, 042315 (2003).

[5] F. G. Deng and G. L. Long, Phys. Rev. A **70**, 012311 (2004).

[6] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).

[7] I. P. Degiovanni, I. R. Berchera, S. Castelletto, et al., Phys. Rev. A 69, 032310 (2004); A. Wǿjicik, Phys. Rev. A 71, 016301 (2005); I. P. Degiovanni, I. R. Berchera, S. Castelletto, et al., Phys. Rev. A 71, 016302 (2004).

[8] F. G. Deng, G. L. Long and X. S. Liu, Phys. Rev. A **68**, 042317 (2003).

[9] F. G. Deng and G. L. Long, Phys. Rev. A **69**, 052319 (2004).

[10] F. G. Deng and G. L. Long, e-print quant-ph/0408102.

[11] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Phys. Rev. A **71**, 044305 (2005).

[12] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).

[13] Q. Y. Cai and B. W. Li, Phys. Rev. A **69**,054301 (2004).

[14] Q. Y. Cai and B. W. Li, Chin. Phys. Lett. **21**, 601 (2004).

[15] F. L. Yan and X. Zhang, Euro. Phys. Journal. B **41**, 75 (2004).

[16] T. Gao, F. L. Yan and Z. X. Wang, Nuove Cimento Della Societa Italiana Di Fisica B **119** (3), 313 (2004); T. Gao, F. L. Yan and Z. X. Wang, Zeitschrift Fur Naturforschung Section A **59**, 597 (2004).

[17] Z. J. Zhang, Z. X. Man an Y. Li, Phys. Lett. A **333**, 46 (2004); Z. X. Man, Z. J. Zhang and Y. Li, Chin. Phys. Lett. **22**, 18 (2005); Z. X. Man, Z. J. Zhang and Y. Li, Chin. Phys. Lett. **22**, 22 (2005).

[18] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829(1999).

[19] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[20] F. G. Deng, H. Y. Zhou, and G. L. long, Phys. Lett. A **337**, 329 (2005).

[21] F. G. Deng, G. L. Long, and H. Y. Zhou, Phys. Lett. A **340**, 43 (2005).

[22] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).

[23] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).

[24] Y. M. Li, K. S. Zhang, and K. C. Peng, Phys. Lett. A **324**, 420 (2004).

[25] F. G. Deng, X. H. Li, C. Y. Li, P. Zhou and H. Y. Zhou, Phys. Rev. A (in press); e-print quant-ph/0504158.

[26] F. G. Deng, C. Y. Li, Y. S. Li, H. Y. Zhou, and Y. Wang, Phys. Rev. A (in press); e-print quant-ph/0501129.

[27] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Rev. A **71**, 044301 (2005); F. G. Deng, X. H. Li, H. Y. Zhou, and Z. J. Zhang, Phys. Rev. A (in press), e-print quant-ph/0506194.

[28] G. R. Blakley, in *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979), pp.313-317; A. Shamir, Commun. ACM **22**, 612 (1979).

[29] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999); P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[30] Q. Y. Cai, e-print quant-ph/0508002.